REMARKS

The Office Action of September 3, 2008 has been reviewed and the comments therein were carefully considered. Claims 9, 27, 29, and 33-58 are pending with this paper. Claims 9, 27, 29, 43, 44, and 51 are rejected.

Applicant acknowledges that claims 33-42, 45-50, and 52 are objected to as being dependent upon a rejected base claim, but would be allowable if all corresponding objected claims are merged and rewritten in independent form including all of the limitations of the base claim and all intervening claims.

Applicant is adding claims 53-58, which are supported by the specification as originally filed. For example, claims 53, 55, and 57 are supported by Figure 10 and page 16, line 12- page 21, line 8. Claims 54, 56, and 58 are supported by page 7, lines 10-16.

Substance of Interview on November 13, 2008

Applicant and Examiner discussed proposed amendments to claim 9. No agreement was reached.

Claim Rejections Under 35 U.S.C. §102

Claims 9, 27, 29, 43-44, and 51 are rejected under 35 USC 102(e) as allegedly being anticipated by U.S. Patent No. 6,754,713 (Dascalu).

Regarding claim 9, Dascalu fails to even suggest the features of "an authentication component configured to **authenticate** a communicating device" and "an access control component accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication component, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control component configured to instruct the authentication component to **authenticate** the communicating device, wherein the access control component is configured to

receives indications originating from the communicating device identifying the communicating device and the application requested." (Emphasis added.)

Applicant believes that the Office Action has not properly considered the terminology "authenticate" as understood by one of ordinary skill in the art. The specification elaborates on the meaning of "authenticate", *e.g.,* page 6, line 7 - page 7, line 16 and page 17, line 4 - page 18, line 10. A person skilled in the art would understand "an authentication component configured to authenticate a communicating device" to mean a component which checks the authenticity of a communicating device to make sure that the communicating device is genuine. Dascalu does not even disclose such a feature and certainly does not disclose the use of such an authentication component as recited in the claims. It would not be obvious to a person skilled in the art to adapt the teachings of Dascalu and fall within the scope of the independent claims. Dascalu does not teach any authentication functions and would consequently not motivate a person of ordinary skill in the art to adapt the teaching of Dascalu to fall within the scope of the independent claims.

The claimed invention is directed to an apparatus which includes at least a first application 118, an authentication component 106 for authenticating a communicating device, and an access control component 120. (Page 12, line 5 – page 16, line 10.) In operation, the communicating device may contact the access control component 120 of the apparatus and request access to the first application 118. At this stage, the communicating device has not been authenticated by the authentication component 106. The access control component then arbitrates whether access of the communication device to the first application 118 is granted or refused. If the arbitration requires an authentication of the communicating device, the access control component 120 instructs the authentication component 106 to authenticate the communicating device.

The Office Action alleges that Dascalu discloses (Pages 4-5, section 4):

> Regarding Claim 9 teaches and describes a apparatus (Fig.1-3, co1.2 line 20 to co1.3 line 60), comprising: at least a first application; an authentication component configured to authenticate a communicating device; an access control component accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication means, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access

> control component configured instructs the authentication component to authenticate the communicating device, wherein the access control component is configured receives indications originating from the communicating device identifying the communicating device and the application requested (co1.4 line 25 to co1.5 line 67).

However, Dascalu merely discusses a session wall device which is connected to a local area network for passively listening to communications sent over the network and for terminating communication sessions between devices if it detects an event which is not permitted. As illustrated in Fig. 1 of Dascalu, the session wall device is connected to a network 1 via a network adapter 2. The session wall device includes a protocol scanner 16 which scans data in a received data buffer 6 and compares it with access rules 10 to determine whether a message between devices is permitted or not. The access rules 10 are a table of groups of servers, groups of clients and rules between them. The rules define actions which should take place when a specific set of protocols are used when two or more parties communicate. When the protocol scanner 16 detects an event which is not permitted by the access rules 10, the protocol scanner 16 generates a message which terminates the communication session in which that event took place. Dascalu further discusses access rules 10. For example, Dascalu discloses that (Column 5, lines 6-20. Emphasis added.):

> **Access rules 10 mentioned above are a table of groups of servers, groups of clients, and rules between them. The rules define actions which should take place when a specific set of protocols is used when two or more parties communicate, and also, when specific data content, or specific data sequences are passed over the network.** The definition contains several logical and mathematical combinations after which a specific action is to be performed. For example, if a client is connecting to a Telnet server and is using an FTP session on that server, the session wall will issue a command to the Telnet server to terminate the FTP session. Another example is that if a client is limited to two concurrent sessions of Telnet and FTP together and he tries to open a third session, both server and client will get a message that the other party closed the connection in order to inhibit the third session.

Dascalu merely discusses access rules 10 to detect a protocol error (*e.g.,* attempting to establish an FTP session with a Telenet server). However, Dascalu does <u>not</u> discuss any authentication functions. As taught by Dascalu, protocol scanner 16 assumes that it correctly knows which devices are communicating in the session.

Independent claim 27 includes the similar features of "an authentication component configured to authenticate a communicating device," "a first access control component accessible by a communicating device requesting access to the first application without the communicating device having been authenticated by the authentication component, and arranged to arbitrate whether access of the communicating device to the first application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the access control component configured to instruct the authentication component to authenticate the communicating device," and "a second access control component accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication component, and arranged to arbitrate whether access of the communicating device to the second application is granted or refused wherein if the arbitration requires an authentication of the communicating device, the second access control component configured to instruct the authentication component to authenticate the communicating device, wherein the first access control component is accessible by a communicating device requesting access to the second application without the communicating device having been authenticated by the authentication component, and is arranged to provide the access of the communicating device to the second access control component." Also, independent claim 29 includes the feature of "determining, in the arbitration component, whether to grant or refuse access to the first application by the requesting device, wherein if the determination requires an authentication of the requesting device, the authentication is performed during that determination and not previously, wherein the determination is made on the basis of the identity of service requested and/or the identity of the requesting device." Similarly, independent claim 43 includes the feature of "determining, in the arbitration component, whether to grant or refuse access to the application, wherein if the determination requires an authentication of the requesting device, the authentication is performed during that determination and not previously, wherein the determination is made on the basis of the identity of the application requested." Similarly, independent claim 51 includes the feature of "determining, in the arbitration component, whether to grant or refuse access to the application, wherein if the determination requires an authentication of the requesting device, the authentication is performed during that determination and not previously, wherein the determination is made on the basis of

the identity of the application requested." Moreover, claim 44 depends from claim 43 and is not anticipated for at least the above reasons. Applicant requests reconsideration of claims 9, 27, 29, 43-44, and 51.

Because new claims 53-58 depend from claims 9, 27, and 43, claims 53-58 are not anticipated for at least the above reasons. Moreover, Dascalu fails to suggest any thing about a personal identification number or temporary authentication link key.

Applicants therefore respectfully request reconsideration of the pending claims and a finding of their allowability. A notice to this effect is respectfully requested. Please feel free to contact the undersigned should any questions arise with respect to this case that may be addressed by telephone.

Respectfully submitted,

Date: December 3, 2008

By: /Kenneth F. Smolik/
Kenneth F. Smolik
Registration No. 44,344
BANNER & WITCOFF, LTD.
10 South Wacker Drive
Suite 3000
Chicago, Illinois 60606
Phone: 312-463-5000
Fax: 312-463-5001